REMARKS/ARGUMENTS

These remarks are submitted in response to the Office Action of February 4, 2008 (Office Action). As this response is timely filed within the 3-month shortened statutory period, no fee is believed due. However, the Examiner is expressly authorized to charge any deficiencies or credit any overpayments to Deposit Account 50-0951.

Claim Rejections – 35 USC § 103

In the Office Action, Claims 1-18 and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Published Patent Application 2003/0217137 to Roese (hereinafter Roese) in view of U.S. Published Patent Application 2003/0115481 to Baird (hereinafter Baird).

Although Applicants respectfully disagree with the claim rejections, Applicants have amended the claims so as to expedite prosecution of the present application. It is expressly noted, however, that the amendments should not be interpreted as the surrender of any subject matter. Accordingly, Applicants respectfully reserve the right to present the original version of any of the amended claims in any future divisional or continuation applications from the present application.

Applicants have amended independent Claims 1, 7, and 13 to further emphasize certain aspects of the invention. As discussed herein, the claim amendments are fully supported throughout the Specification. No new matter has been introduced by the claim amendments.

Certain Aspects Of Applicants' Invention

At this juncture, it may be helpful to reiterate certain aspects of Applicants' invention. One embodiment of the invention, typified by Claim 1, is a method for managing a presentation of sensitive content in non-trusted environments.

The method can include interrogating a list of one or more corporate policies associated with a given user and with a physical device. The policy data can be acquired locally from the physical device or dynamically via access to a corporate network. Each corporate policy prohibits or restricts access to corporate data in a non-trusted environment. The method also can include determining a location of the physical device, and determining whether the user and the physical device is in a trusted or non-trusted environment by comparing the location of the physical device with a list of trusted locations. The list of trusted locations can be embedded within the policy data or stored separately. (See, e.g., Specification, paragraphs [0011] to [0013].)

The method also can include providing access to a subscription-based service, which maintains an organization list comprising individuals and machine identification information. The organization list can identify and indicate that a particular individual or machine listed is associated with a predetermined competitive organization. The method further can include determining that an individual or machine identified on the list associated with the competitive organization is within a predetermined proximity of the physical device. Further according to the method, if it is determined that an individual or machine identified on the list is within a predetermined proximity of the physical device, then an alert can be transmitted to a user via the physical device. (See, e.g., Specification, paragraph [0019].)

Additionally, the method can include enforcing a plurality of rules contained in the policy for managing the presentation of sensitive content. More particularly, the rules can be enforced by blocking a visual presentation or audible presentation of at least one object in portions of the presentation if (1) the physical device is not located in a trusted location, or (2) an individual or a machine identified on the competitive organization list is within a predetermined proximity of the physical device. (See, e.g., Specification, paragraph [0014].)

The Claims Define Over The References

Roese discloses a method of determining a physical location of a client device requesting access to a data network infrastructure by one or more trusted network devices within the data network infrastructure. However, Roese does not disclose interrogating a list of one or more corporate policies associated with a given user and a physical device, as recited in independent Claims 1, 7, and 13 of the instant application. It is not clear how step 425 -- "Is user authenticated to access requested information/application?" -- in Fig. 4 has anything to do with interrogating a list of one or more corporate policies associated with a given user and a physical device. It is noted that authentication (using password, access card, or fingerprint; see Specification, paragraph [0015], lines 8-15) is different from interrogation of a list of one or more corporate policies to determine the relevant policy that dictates how sensitive content should be displayed in a non-trusted environment.

Roese also does not disclose using a subscription-based service to detect individuals or devices associated with a competitive organization and alerting the user when such an individual or device of the competitive organization is within a predetermined proximity of the user's physical device, as recited in independent Claims 1, 7, and 13 of the instant application. Roese describes in paragraph [0104] that the network can halt the authentication process, sound alarms and/or report the location of the unauthorized user if the user fails to meet the security lever associated with that particular location. However, Roese does not disclose alerting the user when an individual or device of a competitive organization is within a predetermined proximity of the user's physical device.

Baird does not make up for the deficiencies of Roese.

Accordingly, the cited references, alone or in combination, fail to disclose or suggest each and every element of Claims 1, 7, and 13, as amended. Applicants therefore respectfully submit that amended Claims 1, 7, and 13 define over the prior art.

Furthermore, as each of the remaining claims depends from Claim 1, 7, or 13 while reciting additional features, Applicants further respectfully submit that the remaining claims likewise define over the prior art.

Applicants thus respectfully request that the claims rejections under 35 U.S.C. § 103 be withdrawn.

CONCLUSION

Applicants believe that this application is now in full condition for allowance, which action is respectfully requested. Applicants request that the Examiner call the undersigned if clarification is needed on any matter within this Amendment, or if the Examiner believes a telephone interview would expedite the prosecution of the subject application to completion.

Respectfully submitted,

Date: May 5, 2008

/Richard A. Hinson/
Gregory A. Nelson, Registration No. 30,577
Richard A. Hinson, Registration No. 47,652
Yonghong Chen, Registration No. 56,150
AKERMAN SENTERFITT
Customer No. 40987
Post Office Box 3188
West Palm Beach, FL 33402-3188
Telephone: (561) 653-5000